Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 30 août 2000
N° CERTA-2000-AVI-038

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sous ISS REAL SECURE

Gestion du document

Référence	CERTA-2000-AVI-038
Titre	Vulnérabilité sous ISS REAL SECURE
Date de la première version	30 août 2000
Date de la dernière version	–
Source(s)	Bugtraq
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Contournement des détections d'attaques ;
- Déni de service.

2 Systèmes affectés

- RealSecure 3.2.1 sous Solaris ;
- RealSecure 3.2.2 sous Solaris ;
- RealSecure 3.2.1 sous Windows NT.

3 Résumé

Une vulnérabilité dans le moteur réseau d'ISS RealSecure permet d'arrêter l'agent responsable du contrôle des paquets du réseau.

4 Description

ISS RealSecure est un logiciel permettant une surveillance du trafic réseau, par le biais d'un agent de réseau, dans le but de découvrir des signatures d'attaques.

Une vulnérabilité sur le traitement des paquets ayant l'indicateur SYN a été découverte dans cet agent de réseau entraînant l'arrêt du moteur réseau.

Sous Solaris, l'arrêt du moteur est signifié à la console traitant les données du moteur et des agents.

Sous NT, le moteur se relance juste après avoir été arrêté, provoquant ainsi 100 % d'activité CPU.

5 Contournement provisoire

Aucun correctif n'est actuellement disponible auprès de l'éditeur. Cependant la désactivation de la détection d'attaque par SynFlood et IPFrag contourne cette vulnérabilité mais laisse le réseau vulnérable sur ce type d'attaque.

6 Documentation

Aucune documentation actuellement disponible.

Gestion détaillée du document

30 août 2000 version initiale.